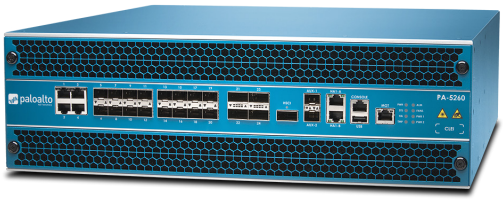
## Highlights

- World's first ML-Powered NGFW
- Nine-time Leader in the Gartner Magic Quadrant® for Network Firewalls
- Leader in The Forrester Wave™: Enterprise Firewalls, Q3 2020
- Highest Security Effectiveness score in the 2019 NSS Labs NGFW Test Report, with 100% of evasions blocked
- Delivers 5G-native security built to safeguard service provider and enterprise 5G transformation and multi-access edge computing (MEC)
- Extends visibility and security to all devices, including unmanaged IoT devices, without the need to deploy additional sensors
- Supports high availability with active/active and active/passive modes
- Delivers predictable performance with security services

# PA-5200 Series



PA-5260

Palo Alto Networks PA-5200 Series ML-Powered NGFWs—the PA-5280, PA-5260, PA-5250, and PA-5220—are ideal for high-speed data center, internet gateway, and service provider deployments. The PA-5200 Series delivers up to 64 Gbps of throughput, using dedicated processing and memory, for the key functional areas of networking, security, threat prevention, and management.

The world's first ML-Powered Next-Generation Firewall (NGFW) enables you to prevent unknown threats, see and secure everything—including the Internet of Things (IoT)—and reduce errors with automatic policy recommendations. The controlling element of the PA-5200 Series is PAN-OS®, the same software that runs all Palo Alto Networks NGFWs. PAN-OS natively classifies all traffic, inclusive of applications, threats, and content, and then ties that traffic to the user regardless of location or device type. The application, content, and user—in other words, the elements that run your business—then serve as the basis of your security policies, resulting in improved security posture and reduced incident response time.

## Key Security and Connectivity Features

### ML-Powered Next-Generation Firewall

- Embeds machine learning (ML) in the core of the firewall to provide inline signatureless attack prevention for file-based attacks while identifying and immediately stopping never-before-seen phishing attempts.
- Leverages cloud-based ML processes to push zero-delay signatures and instructions back to the NGFW.
- Uses behavioral analysis to detect IoT devices and make policy recommendations; cloud-delivered and natively integrated service on the NGFW.
- Automates policy recommendations that save time and reduce the chance of human error.

### Identifies and categorizes all applications, on all ports, all the time, with full Layer 7 inspection

- Identifies the applications traversing your network irrespective of port, protocol, evasive techniques, or encryption (TLS/SSL).
- Uses the application, not the port, as the basis for all your safe enablement policy decisions: allow, deny, schedule, inspect, and apply traffic-shaping.
- Offers the ability to create custom App-ID™ tags for proprietary applications or request App-ID development for new applications from Palo Alto Networks.
- Identifies all payload data within the application (e.g., files and data patterns) to block malicious files and thwart data exfiltration attempts.
- Creates standard and customized application usage reports, including software-as-a-service (SaaS) reports that provide insight into all sanctioned and unsanctioned SaaS traffic on your network.
- Enables safe migration of legacy Layer 4 rule sets to App-ID-based rules with built-in Policy Optimizer, giving you a rule set that is more secure and easier to manage.

### Enforces security for users at any location, on any device, while adapting policy based on user activity

- Enables visibility, security policies, reporting, and forensics based on users and groups—not just IP addresses.
- Easily integrates with a wide range of repositories to leverage user information: wireless LAN controllers, VPNs, directory servers, SIEMs, proxies, and more.
- Allows you to define Dynamic User Groups (DUGs) on the firewall to take time-bound security actions without waiting for changes to be applied to user directories.
- Applies consistent policies irrespective of users' locations (office, home, travel, etc.) and devices (iOS and Android® mobile devices, macOS®, Windows®, Linux desktops, laptops; Citrix and Microsoft VDI and Terminal Servers).
- Prevents corporate credentials from leaking to third-party websites and prevents reuse of stolen credentials by enabling multi-factor authentication (MFA) at the network layer for any application without any application changes.
- Provides dynamic security actions based on user behavior to restrict suspicious or malicious users.

### Prevents malicious activity concealed in encrypted traffic

- Inspects and applies policy to TLS/SSL-encrypted traffic, both inbound and outbound, including for traffic that uses TLS 1.3 and HTTP/2.
- Offers rich visibility into TLS traffic, such as amount of encrypted traffic, TLS/SSL versions, cipher suites, and more, without decrypting.
- Enables control over use of legacy TLS protocols, insecure ciphers, and misconfigured certificates to mitigate risks.
- Facilitates easy deployment of decryption and lets you use built-in logs to troubleshoot issues, such as applications with pinned certificates.
- Lets you enable or disable decryption flexibly based on URL category and source and destination zone, address, user, user group, device, and port, for privacy and regulatory compliance purposes.
- Allows you to create a copy of decrypted traffic from the firewall (i.e., decryption mirroring) and send it to traffic collection tools for forensics, historical purposes, or data loss prevention (DLP).

### Offers centralized management and visibility

- Benefits from centralized management, configuration, and visibility for multiple distributed Palo Alto Networks NGFWs (irrespective of location or scale) through Panorama™ network security management, in one unified user interface.
- Streamlines configuration sharing through Panorama with templates and device groups, and scales log collection as logging needs increase.
- Enables users, through the Application Command Center (ACC), to obtain deep visibility and comprehensive insights into network traffic and threats.

### Detects and prevents advanced threats with cloud-delivered security services

Today's sophisticated cyberattacks can spawn 45,000 variants in 30 minutes using multiple threat vectors and advanced techniques to deliver malicious payloads. Traditional siloed security causes challenges for organizations by introducing security gaps, increasing overhead for security teams, and hindering business productivity with inconsistent access and visibility.

Seamlessly integrated with our industry-leading NGFWs, our Cloud-Delivered Security Services use the network effect of

80,000 customers to instantly coordinate intelligence and protect against all threats across all vectors. Eliminate coverage gaps across your locations and take advantage of best-in-class security delivered consistently in a platform to stay safe from even the most advanced and evasive threats. Services include:

- **Threat Prevention**—goes beyond a traditional intrusion prevention system (IPS) to prevent all known threats across all traffic in a single pass without sacrificing performance.
- **Advanced URL Filtering**—provides best-in-class web protection while maximizing operational efficiency with the industry's first real-time web protection engine and industry-leading phishing protection.
- **WildFire®**—ensures files are safe with automatic detection and prevention of unknown malware powered by industry-leading cloud-based analysis and crowdsourced intelligence from more than 42,000 customers.
- **DNS Security**—harnesses the power of ML to detect as well as prevent threats over DNS in real time and empowers security personnel with the intelligence and context to craft policies and respond to threats quickly and effectively.
- **IoT Security**—provides the industry's most comprehensive IoT security solution, delivering ML-powered visibility, prevention, and enforcement in a single platform.
- **Enterprise DLP**—offers the industry's first cloud-delivered enterprise DLP that consistently protects sensitive data across networks, clouds, and users.
- **SaaS Security**—delivers integrated SaaS security that lets you see and secure new SaaS applications, protect data, and prevent zero-day threats at the lowest total cost of ownership (TCO).

## Delivers a unique approach to packet processing with Single-Pass Architecture

- Performs networking, policy lookup, application and decoding, and signature matching—for all threats and content—in a single pass. This significantly reduces the amount of processing overhead required to perform multiple functions in one security device.
- Avoids introducing latency by scanning traffic for all signatures in a single pass, using stream-based, uniform signature matching.
- Enables consistent and predictable performance when security subscriptions are enabled. (In table 1, "Threat Prevention throughput" is measured with multiple subscriptions enabled.)

## Enables SD-WAN functionality

- Allows you to easily adopt SD-WAN by simply enabling it on your existing firewalls.
- Enables you to safely implement SD-WAN, which is natively integrated with our industry-leading security.
- Delivers an exceptional end user experience by minimizing latency, jitter, and packet loss.

**Table 1: PA-5200 Series Performance and Capacities**

| | PA-5280 | PA-5260 | PA-5250 | PA-5220 |
|---|---|---|---|---|
| Firewall throughput (HTTP/appmix)* | 54.2/60.0 Gbps | 54.2/60.0 Gbps | 35.7/37.3 Gbps | 15.2/17 Gbps |
| Threat Prevention throughput (HTTP/appmix)† | 27.1/33.8 Gbps | 27.1/33.8 Gbps | 18.3/23.0 Gbps | 7.7/9.7 Gbps |
| IPsec VPN throughput‡ | 28 Gbps | 28 Gbps | 19 Gbps | 9.7 Gbps |
| Max sessions | 64M | 32M | 8M | 4M |
| New sessions per second§ | 586,000 | 586,000 | 392,000 | 166,000 |
| Virtual systems (base/max)\|\| | 25/225 | 25/225 | 25/125 | 10/20 |

Note: Results were measured on PAN-OS 10.1.

* Firewall throughput is measured with App-ID and logging enabled, utilizing 64 KB HTTP/appmix transactions.

† Threat Prevention throughput is measured with App-ID, IPS, antivirus, anti-spyware, DNS Security, WildFire, file blocking, and logging enabled, utilizing 64 KB HTTP/appmix transactions.

‡ IPsec VPN throughput is measured with 64 KB HTTP transactions and logging enabled.

§ New sessions per second is measured with application-override, utilizing 1 byte HTTP transactions.

|| Adding virtual systems over base quantity requires a separately purchased license.

**Table 2: PA-5200 Series Networking Features**

| Interface Modes |
|---|
| L2, L3, tap, virtual wire (transparent mode) |
| **Routing** |
| OSPFv2/v3 with graceful restart, BGP with graceful restart, RIP, static routing |
| Policy-based forwarding |
| Point-to-point protocol over Ethernet (PPPoE) and DHCP supported for dynamic address assignment |
| Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3 |
| Bidirectional Forwarding Detection (BFD) |

**Table 2: PA-5200 Series Networking Features (cont.)**

| SD-WAN |
|---|
| Path quality measurement (jitter, packet loss, latency) |
| Initial path selection (PBF) |
| Dynamic path change |
| **IPv6** |
| L2, L3, tap, virtual wire (transparent mode) |
| Features: App-ID, User-ID, Content-ID, WildFire, and SSL Decryption |
| SLAAC |

| Table 2: PA-5200 Series Networking Features (cont.) |
|---|
| **IPsec VPN** |
| Key exchange: manual key, IKEv1 and IKEv2 (pre-shared key, certificate-based authentication) |
| Encryption: 3DES, AES (128-bit, 192-bit, 256-bit) |
| Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512 |
| GlobalProtect large-scale VPN for simplified configuration and management |
| **VLANs** |
| 802.1Q VLAN tags per device/per interface: 4,094/4,094 |
| Aggregate interfaces (802.3ad), LACP |
| **Network Address Translation** |
| NAT modes (IPv4): static IP, dynamic IP, dynamic IP and port (port address translation) |
| NAT64, NPTv6 |
| Additional NAT features: dynamic IP reservation, tunable dynamic IP and port oversubscription |
| **High Availability** |
| Modes: active/active, active/passive, HA clustering |
| Failure detection: path monitoring, interface monitoring |
| **Mobile Network Infrastructure*** |
| GTP Security |
| SCTP Security |

* For additional information, refer to our ML-Powered NGFWs for 5G datasheet.

| Table 3: PA-5200 Series Hardware Specifications |
|---|
| **I/O** |
| PA-5280 / PA-5260 / PA-5250: 100/1000/10G Cu (4), 1G/10G SFP/ SFP+ (16), 40G/100G QSFP28 (4)<br>PA-5220: 100/1000/10G Cu (4), 1G/10G SFP/SFP+ (16), 40G QSFP+ (4) |
| **Management I/O** |
| PA-5280 / PA-5260 / PA-5250: 10/100/1000 (2), 40G/100G QSFP28 HA (1), 10/100/1000 out-of-band management (1), RJ45 console port (1) |
| PA-5220: 10/100/1000 (2), 40G QSFP+ HA (1), 10/100/1000 out-of-band management (1), RJ45 console port (1) |
| **Storage Capacity** |
| 240 GB SSD, RAID1, system storage<br>2 TB HDD, RAID1, log storage |

| Table 3: PA-5200 Series Hardware Specifications (cont.) |
|---|
| **Power Supply (Avg/Max Power Consumption)** |
| 571/685 W |
| **Max BTU/hr** |
| 2,340 |
| **Power Supplies (Base/Max)** |
| 1:1 fully redundant (2/2) |
| **AC Input Voltage (Input Hz)** |
| 100–240 VAC (50–60 Hz) |
| **AC Power Supply Output** |
| 1,200 watts/power supply |
| **Max Current Consumption** |
| AC: 8.5 A @ 100 VAC, 3.6 A @ 240 VAC<br>DC: 19 A @ -40 VDC, 12.7 A @ -60 VDC |
| **Max Inrush Current** |
| AC: 50 A @ 230 VAC, 50 A @ 120 VAC<br>DC: 200 A @ 72 VDC |
| **MTBF** |
| 9.23 years |
| **Rack Mount (Dimensions)** |
| 3U, 19” standard rack<br>5.25” H x 20.5” D x 17.25” W |
| **Weight (Standalone Device/As Shipped)** |
| 46 lbs/62 lbs |
| **Safety** |
| cTUVus, CB |
| **EMI** |
| FCC Class A, CE Class A, VCCI Class A |
| **Certifications** |
| See paloaltonetworks.com/company/certifications.html |
| **Environment** |
| Operating temperature: 32° to 122° F, 0° to 50° C<br>Non-operating temperature: -4° to 158° F, -20° to 70° C |

To view additional information about the features and associated capacities of the PA-5200 Series, please visit paloaltonetworks.com/network-security/next-generation-firewall/pa-5200-series.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com